NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY

Volume 20
Issue 5 *Online Issue*

Article 8

5-1-2019

Someone Else May Own a Piece of You: Lack of Federal Regulation over Direct-to-Consumer DNA Test Kits

Alexander (Zan) Eric Newkirk

NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY
VOLUME 20, ISSUE ON.2: MAY 2019

SOMEONE ELSE MAY OWN A PIECE OF YOU: LACK OF FEDERAL REGULATION OVER DIRECT-TO-CONSUMER DNA TEST KITS

Alexander (Zan) Eric Newkirk*

Direct-to-consumer DNA test kits, such as those sold by Ancestry and 23andMe, are now more popular than ever. These test kits require a consumer to submit a personal DNA sample in exchange for detailed results about the consumer's ancestry. Although about half of the United States has a genetic privacy law, they vary in strictness and applicability to direct-to-consumer DNA test kits. There is currently no federal law regulating the test kit companies' control over the DNA samples they collect, leaving the direct-to-consumer DNA test kit industry largely self-regulated. The company policies which regulate their own control over consumer DNA can leave room for interpretation about the limits of such control. This lack of clear government oversight, in addition to the inherent value of consumer DNA, creates a strong demand for an all-encompassing federal law that creates uniform collection, storage, and use of genetic information. Analysis of state genetic privacy laws provides a building block upon which an effective federal genetic privacy law can be constructed.

* J.D. Candidate, University of North Carolina School of Law, 2020. Thank you, NC JOLT editors, for your insightful feedback. I would also like to express my gratitude to my family for their constant love and support, and the Appalachian State University Department of Chemistry, where I received my B.S., for furthering my interest in science and the law.

I. INTRODUCTION

The twenty-first century has witnessed an expansion of societal interest from safekeeping tangible assets—such as the home, cash, and family—to protecting intangible assets as well, such as online bank accounts, social media, and even individual genetic identifiers. Americans often secure their Facebook profiles with case-sensitive passwords that require a number *and* a symbol to prevent unauthorized users from gaining access.[1] Most online accounts even require that users answer highly intrusive and personal security questions as a secondary method of access to the account in the case the user in question forgets their login information.[2] While Twitter

[1] *See How Can I Make My Facebook Password Strong?*, FACEBOOK, https://www.facebook.com/help/124904560921566?helpref=popular_topics (last visited Jan. 27, 2019).

[2] *See, e.g.*, *How to Update Your Security Questions & Answers*, FIDELITY, https://www.fidelity.com/customer-service/how-to-change-your-security-questions-and-answers (last visited Jan. 27, 2019) ("Security questions help

and electronic banking sites have ramped up their defenses, deoxyribonucleic acid ("DNA") testing kits with limited data security have swept the nation, leaving some test kit users' personal genetic information accessible to others.

Direct-to-consumer ("DTC") genetic testing kits are marketed—often through the internet—directly to the consumer, who sends a DNA sample back to the testing kit company for analysis.[3] The company processes the DNA sample and sends the consumer the results, which can include information about a person's ancestry, potential health issues, and more.[4] Ancestry (or genealogical) testing is considered a form of DTC genetic testing.[5] The quality of these at-home test kits varies,[6] but some of the more well-known brands perform an intricate analysis of the consumer's DNA sample. For example, AncestryDNA[7] ("Ancestry") analyzes all 22 pairs of non-sex chromosomes, providing a broad look at the consumer's entire family tree.[8]

The popularity of these DTC genetic testing kits has exploded in recent years, and the trend is expected to continue.[9] By the end of

---

Fidelity ensure it's really you accessing your account."); *The Reason for Security Questions*, SIRIUSXM, http://siriusxmca.custhelp.com/app/answers/detail/a_id/177/~/the-reason-for-security-questions (last visited Jan. 27, 2019) ("Your personal security questions help us verify your identity when you can't remember your username or password.").

[3] *See What is Direct-to-Consumer Genetic Testing?*, U.S. NAT'L LIBR. OF MED.: GENETICS HOME REF. (Apr. 2, 2019), https://ghr.nlm.nih.gov/primer/dtcgenetictesting/directtoconsumer.

[4] *See id.*

[5] *Id.*

[6] *See id.*

[7] ANCESTRYDNA, https://www.ancestry.com (last visited Apr. 21, 2019).

[8] ANCESTRYDNA, ANCESTRYDNA 101: THE INSIDER'S GUIDE TO DNA 2, https://www.ancestrycdn.com/support/us/2016/11/ancestrydna101.pdf.

[9] *See Direct-to-Consumer Genetic Testing Market to Hit $2.5 Bn by 2024: Global Market Insights, Inc.*, PRNEWSWIRE (Dec. 11, 2018, 6:00 AM) [hereinafter *Global Market Insights*], https://www.prnewswire.com/news-releases/direct-to-consumer-genetic-testing-market-to-hit-2-5-bn-by-2024-global-market-insights-inc--830436085.html; *see also* Leah Larkin, *DNA Tests*, DNA GEEK, https://thednageek.com/dna-tests/ (last visited Apr. 5, 2019) (displaying a graph in which less than 2.5 million people were in AncestryDNA's consumer database as of April 2016, whereas approximately 15 million people were in the same database in 2019).

2017, over twelve million consumers had submitted a DNA sample through an at-home genetic testing kit.[10] Ancestry, the leading genealogy company, processed the DNA of more than seven million people in that year.[11] The runner-up in the competitive DTC genetic testing market, 23andME, analyzed over three million DNA samples.[12] The concentrated market of DTC genetic testing requires heavy promotion to stand out. Ancestry spent approximately $109 million on television and other ads in the United States in 2016.[13] 23andME totaled $21 million on advertisements that same year.[14] As advertising and technology advance, the DTC genetic testing industry is expected to soar in value—with an estimated net worth of over $2.5 billion by 2024.[15]

Ancestry[16] prides itself on providing a comprehensive report of a consumer's recent genetic and ancestral history.[17] But sales of Ancestry DTC genetic testing kits are driven by many other factors, such as the desire to know risks for certain genetic diseases[18] and the desire to connect with long-lost relatives.[19] Even when serious

---

[10] Antonio Regalado, *2017 Was the Year Consumer DNA Testing Blew Up*, MIT TECH. REV. (Feb. 12, 2018), https://www.technologyreview.com/s/610233/2017-was-the-year-consumer-dna-testing-blew-up/.

[11] *Id.*

[12] *Id.*

[13] *See id.*

[14] *Id.*

[15] *Global Market Insights*, *supra* note 9.

[16] As Ancestry dominates the DTC genetic testing market, the scope of this article will be narrowed to discuss only Ancestry, not other companies in the same industry.

[17] *AncestryDNA – Frequently Asked Questions (United States)*, ANCESTRYDNA, https://www.ancestry.com/dna/en/legal/us/faq (last visited Jan. 19, 2019).

[18] *See, e.g.*, *Global Market Insights*, *supra* note 9 ("Predictive tests enables [sic] identification of genetic mutation before actual manifestation resulting in early disease diagnosis. Diagnosis of chronic disease such as cancer at an early stage can make significant improvements in the lives of cancer patients resulting in reduced morbidity, greater probability of surviving and less expensive treatment.").

[19] *See, e.g.*, John D'Anna, *Here's Five Things You Need to Know Before You Take a Home DNA Test*, AZCENTRAL (Dec. 23, 2018, 5:00 AM), https://www.azcentral.com/story/news/local/arizona-best-reads/2018/12/23/dna-testing-privacy-what-know-before-home-genealogy-test-ancestry-23-andme-

motives such as these are involved, the privacy policy is likely an afterthought for a consumer.[20] But this privacy policy isn't just any other run-of-the-mill privacy policy.[21] Ancestry's privacy policy is contracting away consumers' rights to arguably the most personal asset a human has—their genetic information. As of this article's publication, there is no federal law regulating the storage, disclosure, and use of this genetic information.[22]

The need for a uniform, all-encompassing federal law that regulates collection, storage, and use of genetic information is urgent. DTC genetic testing kits continue to rise in popularity while collecting, storing, and using Americans' DNA without federal limitation. In Section II, this Recent Development covers Ancestry's privacy policy and the limits the company places on itself when using consumers' genetic information. Section III discusses governmental use of DTC genetic test results. Section IV reflects on the current legal landscape regulating use of genetic information. Lastly, Section V describes the features of a viable federal statute which would place external limits on DTC genetic testing companies' use of their consumers' information.

---

golden-state-killer/2381500002/ (recommending potential DTC genetic testing kit users purchase a kit from "the company with the largest number of samples in its database, Ancestry," to find genetic matches with long-lost relatives).

[20] *See generally* Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J.L. & POL'Y FOR INFO. SOC'Y 543, 543–68 (2008) (stating privacy policies are "read infrequently," and estimating Americans would spend 67.1 billion hours per year reading privacy policies word-for-word, if they were actually read on every website a person encountered).

[21] *See* CARLOS JENSEN & COLIN POTTS, PRIVACY POLICIES EXAMINED: FAIR WARNING OR FAIR GAME? 1 (2003), ftp://ftp.cc.gatech.edu/pub/gvu/tr/2003/03-04.pdf ("[Privacy] policies are in many ways modeled after software license statements."). *But see* Wendy Zamora, *What DNA Testing Kit Companies Are Really Doing with Your Data*, MALWAREBYTES LABS (Nov. 28, 2018), https://blog.malwarebytes.com/101/2018/11/dna-testing-kit-companies-really-data/ (describing the development of privacy policies for DNA testing companies as "pioneering work").

[22] *See Genetic Information Privacy*, ELEC. FRONTIER FOUND., https://www.eff.org/issues/genetic-information-privacy (last visited Jan. 19, 2019) (addressing the fact HIPAA only regulates "covered entities," and pointing out that Ancestry is one of many non-covered entities which collects genetic information).

II. ANCESTRYDNA PRIVACY POLICY

At nine pages long, Ancestry's privacy policy is surprisingly brief, considering the profound privacy interest involved in genetic testing.[23] The most recent update to the Ancestry privacy policy emphasizes transparency, simplicity, and control of the data by the consumer.[24] The policy is prefaced with a few statements of reassurance to address potential concerns of Ancestry consumers, including: the fact that consumers may make unexpected discoveries (i.e. discovering your mother is not your genetic relative, thus not your actual mother); the ability to manage and delete DNA and DNA data as described in the privacy policy; and a reminder to remain confident in Ancestry's use of consumers' data.[25] This last statement raises the question as to why would someone be worried about how their personal data is being used.

A. *Evolution of the Ancestry Privacy Policy*

Ancestry began selling DTC genetic test kits in 2002, sixteen years after the introduction of its website;[26] hence, its privacy policy was not originally prepared to dictate how consumer DNA data was managed or disclosed. The current privacy policy is a part of a constantly evolving agreement that has been shaped in part by public criticism.[27] In the October 14, 2016 update to the Ancestry privacy policy, the company stated, "we cannot guarantee and we do not warrant that loss, misuse, or alteration of data will not occur, and we are not responsible for the theft, destruction, or inadvertent disclosure of your information."[28] In May 2017, a consumer

---

[23] *See* Zamora, *supra* note 21 (mentioning a comprehensive DNA testing company privacy policy that is twenty-one pages long). For the full text of the Ancestry privacy policy, see *Your Privacy*, ANCESTRYDNA, https://www.ancestry.com/cs/legal/privacystatement (last visited Jan. 19, 2019).

[24] *See Your Privacy*, *supra* note 23.

[25] *See id.*

[26] *See Our Story*, ANCESTRYDNA, https://www.ancestry.com/corporate/about-ancestry/our-story (last visited Jan. 19, 2019).

[27] *See* Eric Heath, *Setting the Record Straight: Ancestry and Your DNA*, ANCESTRYDNA (May 21, 2017), https://blogs.ancestry.com/ancestry/2017/05/21/setting-the-record-straight-ancestry-and-your-dna/.

[28] *Ancestry Privacy Statement*, ANCESTRYDNA (Dec. 5, 2017), https://www.ancestry.com/cs/legal/privacystatement

protection litigator in New Jersey claimed that Ancestry's privacy policy and terms of service awarded the company an ownership interest in the consumers' DNA sample in perpetuity, while the consumers' ownership was measured only in years.[29] Immediately after publication of the New Jersey attorney's statement, Eric Heath, Chief Privacy Officer of Ancestry, addressed those claims in a blog post, which included a link to the updated Ancestry terms and conditions.[30] Heath ended his address to the public stating "[Ancestry has] language throughout the process of activating a test that clarifies and limits what [Ancestry] can and can't do with [the consumer's] data" because consumer genomics "is still a new industry."[31] There is no clarification in the blog post about what "test" Heath references or how the "test" sets limits on consumer data disclosure. The public response by one of Ancestry's top personnel demonstrates that Ancestry, and not some external force—such as federal government, restricts the level of ownership by the consumer and the company in the consumer's DNA sample. Ancestry also sets forth in its privacy policy when a consumer's personal information, including genetic data, may be shared with another person.[32] These circumstances are discussed in-depth below.

B. *Circumstances Under Which a User's Personal Information may be Shared*

Although some consumers may believe that the submission of their DNA was just a quick "in-and-out" experiment, the DNA sample can remain in possession of Ancestry indefinitely.[33] After the DNA sample has been processed, the DNA and saliva are de-identified (removed of the individual's name and other identifying markers) and stored in an encrypted database for consumer

---

[https://web.archive.org/web/20171205204523/https://www.ancestry.com/cs/legal/privacystatement].

[29] *See* Joel Winston, *Ancestry.com Takes DNA Ownership Rights from Customers and Their Relatives*, THINKPROGRESS (May 17, 2017, 7:54 PM), https://thinkprogress.org/ancestry-com-takes-dna-ownership-rights-from-customers-and-their-relatives-dbafeed02b9e/.

[30] *See* Heath, *supra* note 27.

[31] *See id.*

[32] *See Your Privacy*, *supra* note 23.

[33] *See id.*

protection.[34] The samples and information are stored so that they are available for "future testing."[35] This future testing is only performed if a customer gives informed consent for further research.[36] The research is executed in collaboration with third-party researchers for the purpose of better understanding "population history, human migration and improv[ing] human health."[37] The third-party researchers include, but are not limited to, academic institutions, non-profits, for-profit businesses, and government agencies.[38] Some of these institutions even provide compensation to Ancestry for the right to access consumer DNA.[39]

Personal information may also be shared when a consumer chooses to share private details with other Ancestry members.[40] This is usually done in order to connect with a "DNA match" who may be a potential relative and to allow members to trade stories about their ancestors and/or personal lives.[41] Personal information may be shared with other service providers whom Ancestry depends on to complete the transaction with the consumer, or if Ancestry is bought out by another company.[42] Service providers of Ancestry generally include laboratory partners, shipping providers, and sample storage facilities.[43] The service providers and any potential acquiring company are also subject to the same privacy policy.[44] Personal information can be shared when Ancestry publishes aggregated data, such as "noting the percentage of immigrants in a state that are

---

[34] *See id. But see* Cassie Martin, *Privacy and Consumer Genetic Testing Don't Always Mix*, SCIENCENEWS (June 5, 2018, 7:00 AM), https://www.sciencenews.org/blog/science-public/privacy-and-consumer-genetic-testing-dont-always-mix (warning that some scientists believe encrypted genetic information may be hacked and decrypted with the use of other publicly-available information).

[35] *See Your Privacy*, *supra* note 23.

[36] *See id.*

[37] *AncestryDNA Informed Consent*, ANCESTRYDNA, https://www.ancestry.com/dna/lp/informedconsent-v4-en (last visited Feb. 16, 2019).

[38] *See id.*

[39] *See id.*

[40] *See Your Privacy*, *supra* note 23.

[41] *See id.*

[42] *See id.*

[43] *See id.*

[44] *See id.*

from a particular geographic region or country".[45] Ancestry follows this statement with a disclaimer that the aggregated data does not provide individual personal information.[46]

Lastly, personal data can be shared when Ancestry believes "it is reasonably necessary to: comply with valid legal process (e.g. subpoenas, warrants); enforce or apply the Ancestry Terms and Conditions; protect the security or integrity of the Services; or protect the rights, property, or safety, or Ancestry, our employees or users."[47] The most available data about any of these circumstantial uses relates to law enforcement requests for user information.[48] Ancestry releases an annual transparency report on how many requests they receive for personal information from law enforcement.[49] In 2017, Ancestry reported granting thirty-one of thirty-four valid requests for information, all of which pertained to investigations involving credit card misuse and identity theft.[50]

III. ACTUAL USE OF DTC GENETIC TEST KIT RESULTS BY LAW ENFORCEMENT

In recent news, DTC genetic test kit results have reportedly been used to help solve murder cold cases and identify dead bodies.[51] One of the primary detective agencies is Parabon NanoLabs ("Parabon"). Parabon does not obtain the genetic data used in solving these cases directly from a DTC genetic test kit company.[52] Rather, Parabon uses the services of GEDmatch, a database of DTC genetic test results voluntarily submitted by users.[53]

---

[45] *See id.*
[46] *See id.*
[47] *Id.*
[48] *See id.*
[49] *See Ancestry 2018 Transparency Report*, ANCESTRYDNA, https://www.ancestry.com/cs/transparency (last visited Jan. 19, 2019).
[50] *Id.*
[51] *See, e.g.*, Kate Snow & Jon Schuppe, *'This is Just the Beginning': Using DNA and Genealogy to Crack Years-Old Cold Cases*, NBC NEWS (July 18, 2018, 4:30 AM), https://www.nbcnews.com/news/us-news/just-beginning-using-dna-genealogy-crack-years-old-cold-cases-n892126.
[52] *See id.*
[53] *See id.*

A. *Parabon's Success*

Parabon has worked with police departments across the nation to make arrests in numerous cold cases and identify deceased individuals.[54] The company advertises this assistance as "Snapshot Genetic Genealogy Service," which "combines new DNA testing methods with genetic and traditional genealogical research to uncover the likely identity of a perpetrator or identify human remains."[55] The Snapshot service was so effective and widely-desired that it closed more than one cold case every two weeks across the United States in its first 100 days of business.[56] Parabon's Chief Genealogist, Cece Moore, describes the Snapshot process as follows:

> [O]nce [Moore] gets a DNA profile from Parabon, [Moore] uploads it into GEDmatch and compiles a list of relatives, narrowing it down to a second or third-cousin, or closer. [Moore] builds the family tree backward to common ancestors—usually the great- or great-great grandparents. Then [Moore] turns forward in time, filling out more branches and narrowing down her search using publicly available data, including obituaries, wedding announcements and social media. [Moore] compiles a list of people who fit the profile of a possible suspect and gives it to police, who take it from there.[57]

This explanation makes clear that a consumer's DTC genetic test kit results can reveal valuable information about the consumer's relatives, who may not have consented to the public display of such material. This caused concern for Curtis Rogers, the founder of GEDmatch, and led him to quickly revise his company's privacy policy to inform patrons they were free to remove their information.[58] Despite this warning, many declined to remove their GEDmatch profile, and the site continues to add approximately 1,500 new profiles a day.[59]

---

[54] *See id.*

[55] *Parabon® Announces 10th Solved Case in First 100 Days of Snapshot® Genetic Genealogy Service*, PARABON NANOLABS (Sept. 18, 2018), https://parabon-nanolabs.com/news-events/2018/09/snapshot-genetic-genealogy-10-solves-in-first-100-days.html.

[56] *Id.*

[57] Snow & Schuppe, *supra* note 51.

[58] *See id.*

[59] *See id.*

A closer look at the revised GEDmatch privacy policy describes a number of ways a patron of GEDmatch can upload "raw" DNA data to the website. Aside from being allowed to upload one's own DNA, GEDmatch allows patrons to upload the:

> DNA of a person who has granted [a patron] specific authorization to upload their DNA to GEDmatch; DNA of a person known by [a patron] to be deceased; and DNA obtained and authorized by law enforcement to either: (1) identify a perpetrator of a violent crime against another individual; or (2) identify remains of a deceased individual[.][60]

The privacy policy defines "violent crime" as homicide or sexual assault, but there is no description of what qualifies as "specific authorization."[61] A few lines down, the privacy policy states "GEDmatch will not be responsible for any raw data provided to GEDmatch in violation of this Policy."[62] This statement is an attempt to remove all liability from the entity that originally made it possible to freely share genetic code among the public. The privacy policy seems to discourage misuse of another person's DTC genetic test results, but the policy does not specify how tightly the company regulates or enforces it.[63]

For example, the policy does not describe the process for confirming that certain DNA was authorized for upload, from a dead individual, or "obtained and authorized by law enforcement" prior to upload on GEDmatch.[64] Nor is there a description of the process for confirming that DNA is being used to "identify a perpetrator of a violent crime" or "identify the remains of a deceased individual."[65] This sheds light on a vulnerability many may not have expected. Without a clear definition of "specific authorization," there is an opportunity for practically anybody who has access to another's DTC genetic test results to upload them on GEDmatch for the world to see. These results could be available to law enforcement, insurance providers, and others who have reason to discriminate

---

[60] *GEDmatch.com Terms of Service and Privacy Policy*, GEDMATCH, https://www.gedmatch.com/tos.htm (last updated May 20, 2018).

[61] *See id.*

[62] *See id.*

[63] *See id.*

[64] *See id.*

[65] *See id.*

against an individual on the basis of their genetic makeup. The policy even states that "future genealogical and non-genealogical uses [of genetic data] may be developed, including uses that GEDmatch cannot predict or foresee[,]"[66] indicating the company hosting these services has no idea how much potential there is for misuse of genetic data. In the absence of any federal law, the only entity capable of preventing potential misuse, the DTC company, has already attempted to remove all liability via its privacy policy. Yet, if companies such as GEDmatch are not held accountable in protecting personal genetic data displayed on their website, then who will?

B. *Legislative Response to Law Enforcement Use of DTC Genetic Test Results*

Some state officials have already taken steps toward holding genealogy databases accountable for any potential misuse of personal genetic data. A Maryland legislator, Charles Sydnor, is advocating for the protection of the public's genetic data from law enforcement.[67] Sydnor believes use of the genealogy databases is an overreach and even a violation of the United States Constitution.[68] Sydnor introduced a bill that would ban law enforcement use of genetic data accessible on genealogy sites, because he believes that just because one person may want to perform a DTC genetic test should not mean that person's extended family is also subject to a search by the state.[69] However, Maryland law enforcement is heavily opposed to the bill and references the successful identification of violent criminals that would not have been possible without police access to genealogy sites.[70]

Although this Maryland bill is not guaranteed to fully protect the public's genetic data from misuse, or guaranteed to even become

---

[66] *Id.*

[67] Lindsay Watts, *Maryland Lawmaker Proposes Bill to Ban Police Use of DNA Databases*, FOX 5 DC (Feb. 11, 2019, 10:22 PM), https://www.fox5dc.com/news/local-news/maryland-lawmaker-proposes-bill-to-ban-police-use-of-dna-databases.

[68] *See id.*

[69] *See id.*

[70] *See id.*

law, it is an attempt to further balance the Fourth Amendment rights of DTC genetic test kit consumers with the urgency of some law enforcement investigations.[71] In urgent situations, such as a homicide or discovery of a dead body, law enforcement will likely want to use all tools available to its investigation. So why shouldn't law enforcement be able to use a DTC genetic test kit consumer's genetic data that was voluntarily posted to a public genealogy site?

C. *Law Enforcement Access to Genetic Data Pursuant to the Third-Party Doctrine*

Public genealogy information that was voluntarily submitted may be accessible by law enforcement pursuant to the third-party doctrine. The third-party doctrine "stems from the notion that an individual has a reduced expectation of privacy in information knowingly shared with another."[72] An individual who shares information with a third party cannot expect the third party to refrain from divulging the information to others, including the government.[73] This allows law enforcement to use information that has been knowingly shared with others.[74] The doctrine originates from two 1970s Supreme Court cases, *Smith v. Maryland* and *United States v. Miller*, and has been most recently re-shaped by *Carpenter v. United States*.[75]

In *Smith*, the Court rejected the defendant's claim that law enforcement's use of a pen register constituted a "search" under the Fourth Amendment because the pen register only kept record of

---

[71] *See id.* (quoting Charles Sydnor, who said, "I may want to perform a DNA search on Ancestry.com, but I don't think that should subject my children and their children and their children's children to a state search.").

[72] Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018).

[73] *See id.* at 2216.

[74] *See generally Carpenter*, 138 S. Ct. 2206 (holding it constitutional for law enforcement to access up to six days'-worth of cell-site records to track the defendant's location over time); Smith v. Maryland, 442 U.S. 735 (1979) (holding law enforcement's use of a pen register to identify the phone number defendant dialed constitutional); United States v. Miller, 425 U.S. 435 (1976) (finding bank notes voluntarily handed over to the bank by the defendant admissible against the defendant).

[75] *Carpenter*, 138 S. Ct. at 2216.

what number was being dialed.[76] The dialed numbers were also given to the telephone company upon making a call.[77] Since the defendant voluntarily informed the telephone company of the numbers he dialed, the defendant no longer had an expectation of privacy as to which numbers he dialed.[78]

In *Miller*, the Court found no legitimate expectation of privacy in the defendant's financial statements which were subpoenaed by law enforcement.[79] The financial statements contained only information which was routinely exposed to employees of the bank.[80] Once the defendant handed this information over to the bank, the defendant assumed the risk that this information could be conveyed to the government.[81]

The Court in *Carpenter* delved deeper into the third-party doctrine to address the fact that technology has advanced far beyond pen registers and bank statements, in turn making a much greater wealth of information available to law enforcement.[82] In this case, the Court found that law enforcement's use of cell-site records to track defendant's location was a "search" within the meaning of the Fourth Amendment.[83] In reaching this conclusion, the Court frequently analogized to the situations at hand in *Smith* and *Miller*.[84] Eventually, the Court drew the following distinction:

> [T]he fact of diminished privacy interests does not mean that the Fourth Amendment falls out of the picture entirely. *Smith* and *Miller*, after all, did not rely solely on the act of sharing. Instead, they considered the

---

[76] *Smith*, 442 U.S. at 742.
[77] *Id.*
[78] *Id.* at 743–44.
[79] *Miller*, 425 U.S. at 442.
[80] *See id.*
[81] *See id.* at 443.
[82] *Carpenter*, 138 S. Ct. at 2223 ("As Justice Brandeis explained in his famous dissent, the Court is obligated—as '[s]ubtler and more far-reaching means of invading privacy have become available to the Government'—to ensure that the 'progress of science' does not erode Fourth Amendment protections. [citation omitted]. Here the progress of science has afforded law enforcement a powerful new tool to carry out its important responsibilities. At the same time, this tool risks Government encroachment of the sort the Framers, 'after consulting the lessons of history,' drafted the Fourth Amendment to prevent.").
[83] *Id.* at 2220.
[84] *See generally id.*

> nature of the particular documents sought to determine whether there is a legitimate expectation of privacy concerning their contents. *Smith* pointed out the limited capabilities of a pen register; . . . telephone call logs reveal little in the way of identifying information. *Miller* likewise noted that checks were not confidential communications but negotiable instruments to be used in commercial transactions.[85]

The Court found the "unique nature of cell phone location information" and the lack of "any affirmative act on the part of the user beyond powering up [the cell phone]" involved privacy issues far greater than those in *Smith* and *Miller*.[86] Although this ruling was a step back from strict adherence to the third-party doctrine, the doctrine remains good law.[87] The Court was careful not to extrapolate the findings in *Carpenter* to future cases which may also present an issue with the third-party doctrine, in fear of "embarrass[ing] the future."[88] In response to Justice Gorsuch's suggestion that the Court address what constitutes a reasonable expectation of privacy in similar situations, the majority responded with "we 'do not begin to claim all the answers today,' and therefore decide no more than the case before us."[89]

In light of this narrow ruling, uncertainty lies ahead for consumers of Ancestry's DTC genetic test kits. With the third-party doctrine still intact, *Carpenter* leaves unclear whether there is any legitimate expectation of privacy in voluntarily-posted genetic data that could provide Fourth Amendment protections from government intrusion. The Court may be waiting for an opportunity to "tread carefully" on the issue once it has all of the relevant facts pertaining to DTC genetic test kits.

If the Court were to grant certiorari to such a case, it would likely analogize the facts of the case to precedent in the same manner as it did in *Carpenter*. Genetic data does not have much in common with the "limited capabilities" of a pen register employed in *Smith*, nor is it comparable to the "negotiable instruments" used in *Miller*.

---

[85] *Id.* at 2219 (internal citations omitted).

[86] *Id.* at 2220.

[87] *See id.* ("[W]e do not disturb the application of *Smith* and *Miller*.").

[88] *Id.* at 2220 ("As Justice Frankfurter noted when considering new innovations in airplanes and radios, the Court must tread carefully in such cases, to ensure that we do not 'embarrass the future.'").

[89] *Id.* at 2220 n.4 (citation omitted).

However, the cell-site records used to track the defendant in *Carpenter* share a bit more in common with genetic data. Whereas the cell-site records are able to locate where an individual is, or has been, genetic data is able to pinpoint the geographical origins of an individual. Since genetic data can be used for much more than simply identifying a person's ancestry, one could reason that genetic information is of an even more "unique nature" than cell-site records, thus Fourth Amendment protections should extend to consumers of DNA genetic test kits. In addition, the lack of any "affirmative act" beyond "powering up" the cell phone could be paralleled to the lack of any affirmative act beyond a consumer "activating" their test kit by submitting their DNA sample.

Following the above reasoning, the Court would presumably rule government access to genetic data on a public domain a "search" within the meaning of the Fourth Amendment. Thus, the third-party doctrine would not excuse law enforcement's unauthorized access of genetic data in the public domain. Nonetheless, this is all speculation into a future scenario in which the Court is presented with a case of genetic data misuse. For the time being, these issues belong solely to the legislature for resolution.

IV. CURRENT REGULATION OF INDIVIDUAL GENETIC INFORMATION

As technology advances and new genealogical innovations are unveiled, the law must follow suit to address whether any restrictions should be set on the use or possession of such technology. This section reveals the flaws in current genetic data protection legislation and focuses on the potential for misuse of this data that could not have possibly been foreseen by legislators enacting these laws. Furthermore, the absence of a federal law which tightly polices the actions of companies in the DTC genetic test kit industry creates an unregulated field of uncertainty. Fortunately, some of the states have established laws that place limits on what DTC genetic test kit companies can do with a person's genetic data.

A. *Genetic Information is Largely Unregulated in the United States*

As of this Recent Development's publication, there remains no uniform, all-encompassing federal law which regulates the collection, storage, or use of genetic data by private or government organizations.[90] States without their own genetic information privacy laws leave their citizens' genetic data protected only by outdated federal privacy laws, whose drafters could not have foreseen the normalized and voluntary collection of individuals' DNA.[91] If state or federal laws such as the Privacy Act of 1974 ("the Privacy Act"), the Family Educational Rights and Privacy Act of 1974 ("FERPA"), the Health Insurance Portability and Accountability Act ("HIPAA"), and the Genetic Information Nondiscrimination Act ("GINA") do not protect the citizens' genetic data, then all discretion lies with the private or government organization in deciding how to collect, store, or use that information.[92] Most of these regulations were intended for a purpose other than protecting citizens from their own voluntarily-submitted DNA from being used against them. For this reason, those laws would not directly apply to companies that handle DTC test kit results nor would the laws govern others' use of the genetic data.

The Privacy Act of 1974 was enacted to prohibit disclosure of records with personal identifiers (such as social security number, name, or birthday) without written consent of the individual to whom the records relate.[93] This statute only restricts the actions of federal agencies and covers only the records controlled by those

---

[90] *See Genetic Information Privacy*, *supra* note 22.

[91] *See* Danny Thakkar, *Biometric Regulations in the U.S. States: The State of Play*, BAYOMETRIC, https://www.bayometric.com/biometric-regulations-us-states/ (last visited Jan. 19, 2019).

[92] *See id*.; *see also Genetic Information Privacy*, *supra* note 22.

[93] *See* Freedom of Info. Act Div., *The Privacy Act*, U.S. DEP'T OF HEALTH & HUMAN SERVS. (Oct. 9, 2018), https://www.hhs.gov/foia/privacy/ index.html; *see also* 5 U.S.C. § 552a (2012) ("Conditions of disclosure. -- No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains . . . .").

agencies.[94] The largest DTC genetic test kit manufacturer, Ancestry, cannot fall within the scope of the Privacy Act as the company is privately-owned.[95]

FERPA was also enacted in 1974[96] to protect the educational records of American students.[97] FERPA applies to any educational institution that receives funding from the United States Department of Education.[98] Since Ancestry is not an educational institution and does not report receiving any funds from the Department of Education, it is unlikely Ancestry is within the scope of FERPA's regulation.

HIPAA was enacted by the United States' government on August 21, 1996, for the purpose of setting a national standard for the protection of certain health information.[99] The regulation

---

[94] *See* Freedom of Info. Act Div., *supra* note 93; *see also* 5 U.S.C. § 552a (defining "agency" as an entity that meets 12 requirements, the first of which is maintaining records required by statute or executive order).

[95] *See Company Facts*, ANCESTRYDNA, https://www.ancestry.com/corporate/about-ancestry/company-facts (last visited Feb. 19, 2019).

[96] *Legislative History of Major FERPA Provisions*, U.S. DEP'T ED. (last modified Feb. 11, 2004), https://www2.ed.gov/policy/gen/guid/fpco/ferpa/leg-history.html; *see also* 20 U.S.C. § 1232g(a)(1)(A) (2012) ("No funds shall be made available under any applicable program to any educational agency or institution which has a policy of denying, or which effectively prevents, the parents of students who are or have been in attendance at a school of such agency or at such institution, as the case may be, the right to inspect and review the education records of their children."); Family Educational Rights and Privacy Act, Pub. L. No. 93-380, § 513(b)(1), 88 Stat. 484 (1974).

[97] *Family Educational Rights and Privacy Act (FERPA)*, U.S. DEP'T ED. (last modified Mar. 1, 2018), https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html?src=rn.

[98] *See id.*; *see also* 20 U.S.C. § 1232g(a)(3) (2012) ("For the purposes of this section the term 'educational agency or institution' means any public or private agency or institution which is the recipient of funds under any applicable program.").

[99] OFFICE FOR CIVIL RIGHTS, U.S. DEP'T OF HEALTH & HUMAN SERVS., SUMMARY OF THE HIPAA PRIVACY RULE 1 (2013); *see also* Health Insurance Portability and Accountability Act, Pub. L. No. 104–191, 110 Stat. 1936 (1996) ("An Act to amend the Internal Revenue Code of 1986 to improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and health care delivery, to promote the use of medical savings accounts, to improve access to long-term care

protects "health information," which includes genetic information,[100] from disclosure by organizations referred to as "covered entities."[101] A "covered entity" is defined as "(1) A health plan[;] (2) A health care clearinghouse[; or] (3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter."[102] None of these definitions would classify Ancestry, or any other DTC genetic test kit manufacturer, as a "covered entity." In certain situations, HIPAA may also apply to a "business associate."[103] But DTC genetic testing companies would not classify as a "business associate" under the Act's definition so long as the company were not working in adjunct with a covered entity.[104] Ancestry states in its

---

services and coverage, to simplify the administration of health insurance, and for other purposes.").

[100] OFFICE FOR CIVIL RIGHTS, U.S. DEP'T OF HEALTH & HUMAN SERVS., HIPAA ADMINISTRATIVE SIMPLIFICATION 14 (2013); *see also* 42 U.S.C. § 1320d-9(a) (2012).

[101] *See* OFFICE FOR CIVIL RIGHTS, *supra* note 99; *see also* § 1320d-1(a).

[102] OFFICE FOR CIVIL RIGHTS, *supra* note 100, at 11; *see also* § 1320d-1(a).

[103] *Id*. at 11. Section 160.102 of the Act, titled "Applicability" states:

> (a) Except as otherwise provided, the standards, requirements, and implementation specifications adopted under this subchapter apply to the following entities:
> (1) A health plan.
> (2) A health care clearinghouse.
> (3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.
> (b) Where provided, the standards, requirements, and implementation specifications adopted under this subchapter apply to a business associate.

[104] *See* OFFICE FOR CIVIL RIGHTS, *supra* note 100, at 11. Section 160.103 of this Act, titled "Definitions," states:

> (3) Business associate includes:
> (i) A Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to protected health information to a covered entity and that requires access on a routine basis to such protected health information.
> (ii) A person that offers a personal health record to one or more individuals on behalf of a covered entity.
> (iii) A subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate.

privacy policy that it does not share genetic information with "insurance companies, employers, or third-party marketers without [the consumer's] express consent"[105]—meaning Ancestry does not work in adjunct with covered entities without the consumer's affirmative consent. Thus, HIPAA does not apply to Ancestry and does not provide any sort of genetic privacy to its consumers.

GINA was enacted on May 21, 2008, to protect citizens from having their genetic information used to discriminate against them in health coverage and employment situations.[106] As stated in the previous paragraph, Ancestry does not share genetic information with either insurance companies or employers without the consumer's informed consent. Consequently, without the informed consent of a consumer, Ancestry does not fall within the scope of GINA. With the exception of GINA, all of these federal laws were enacted before Ancestry began selling DTC genetic test kits.[107] Therefore, lawmakers could not have possibly anticipated the potential for misuse of large amounts of personal genetic data found in databases as large as Ancestry's. The only federal law of interest enacted after the sale of DTC genetic test kits is GINA, but this law was implemented long before the massive surge in popularity of these test kits.[108] GINA also only focuses on the potential for discrimination by an employer or insurer with a person's genetic data, rather than regulating the broader issue of potential for general misuse of personal genetic data. This leaves state legislatures to deal with the issue of implementing laws aimed at preventing general misuse of results from DTC genetic test kits.

B. *State Genetic Privacy Laws Vary in Presence and Rigidity Across the Country*

As of the publication of this Recent Development, only twenty-six states have passed statutes regulating the disclosure of genetic

---

[105] *Ancestry Privacy Statement*, *supra* note 28.

[106] *See Genetic Information*, U.S. DEP'T OF HEALTH & HUMAN SERVS. (June 16, 2017), https://www.hhs.gov/hipaa/for-professionals/special-topics/genetic-information/index.html; *see also* 42 U.S.C. § 2000ff-1(a) (2012).

[107] *See Our Story*, *supra* note26 26 (establishing that Ancestry began selling DTC genetic testing kits in 2002).

[108] *See Global Market Insights*, *supra* note 9.

information.[109] These state laws vary widely in the limits placed upon disclosure and use of other persons' genetic information.[110] There is controversy between commentators as to whether genetic information should be treated the same as other health information.[111] Some commentators agree that it should be regulated in the same manner as non-genetic information, while others argue that genetic information requires special legal protection due to its unique properties—an approach called "genetic exceptionalism."[112] This disagreement among commentators is reflected in the content of the genetic privacy statutes of states across the country.

Some state statutes are narrowly-tailored, similar to federal laws such as GINA, and only prevent disclosure of genetic information in instances where it would affect insurance or employment of an individual.[113] Meanwhile, other states have sweeping policies of genetic information use that require formal and written consent of the individual and restricts law enforcement from obtaining a person's genetic information without that individual's consent.[114] Only five state statutes define a person's genetic information as their

---

[109] *State Genetic Privacy Laws*, NAT'L CONF. ST. LEGISLATURES, http://pierce.wesleyancollege.edu/faculty/hboettger-tong/docs/hbt%20public%20folder/FYS/State%20Genetic%20Summary%20Table%20on%20Privacy%20Laws.htm (last visited Jan. 19, 2019).

[110] *See id.*

[111] *See id.*

[112] *See id.* For a further description of genetic exceptionalism, see AMANDA K. SARATA, CONG. RESEARCH SERV., RL34376, GENETIC EXCEPTIONALISM: GENETIC INFORMATION AND PUBLIC POLICY 1 (2011) ("[Genetic exceptionalism] is based on the supposition that genetic information itself embodies several characteristics that may make it special and differentiate it from other medical or even personal information. According to the perspective of genetic exceptionalism, the characteristics of genetic information that make it different include the following: (1) it can be predictive of future disease; (2) it is a unique identifier; (3) it can reveal information about family members; (4) it is vertically transmitted (passed from parent to child); (5) it can impact communities; (6) it can be used to discriminate and stigmatize; and (7) it can cause serious psychological harm.").

[113] *See, e.g.*, MD. CODE ANN., INS. § 27-909 (West 2019).

[114] *See, e.g.*, HEALTH, SAFETY, AND HOUSING—GENETIC PRIVACY, ALASKA STAT. ANN. § 18.13.010 (West 2019).

own personal property.[115] Alaska is the sole state to define a person's DNA sample as their own personal property.[116] The following analysis will provide a comparison between three different state statutes (Alaska, New Mexico, and Maryland) concerning genetic information privacy.

1. *Alaska*

In 2004, the legislature of Alaska enacted a law regulating genetic privacy.[117] This act is all-encompassing, setting forth an individual's right to their own DNA and how it is collected, stored, or used.[118] The Act requires written consent of an individual, or their

---

[115] *State Genetic Privacy Laws*, *supra* note 109. The five states include Alaska, Colorado, Florida, Georgia, and Louisiana.

[116] *See id*.

[117] *See* § 18.13.010. This section, titled "Genetic testing" states:

> Sec. 18.13.010. Genetic testing.
> (a) Except as provided in (b) of this section,
> (1) a person may not collect a DNA sample from a person, perform a DNA analysis on a sample, retain a DNA sample or the results of a DNA analysis, or disclose the results of a DNA analysis unless the person has first obtained the informed and written consent of the person, or the person's legal guardian or authorized representative, for the collection, analysis, retention, or disclosure;
> (2) a DNA sample and the results of a DNA analysis performed on the sample are the exclusive property of the person sampled or analyzed.
> (b) The prohibitions of (a) of this section do not apply to DNA samples collected and analyses conducted
> (1) under AS 44.41.035 or comparable provisions of another jurisdiction;
> (2) for a law enforcement purpose, including the identification of perpetrators and the investigation of crimes and the identification of missing or unidentified persons or deceased individuals;
> (3) for determining paternity;
> (4) to screen newborns as required by state or federal law;
> (5) for the purpose of emergency medical treatment.
> (c) A general authorization for the release of medical records or medical information may not be construed as the informed and written consent required by this section. The Department of Health and Social Services may by regulation adopt a uniform informed and written consent form to assist persons in meeting the requirements of this section. A person using that uniform informed and written consent is exempt from civil or criminal liability for actions taken under the consent form. A person may revoke or amend their informed and written consent at any time.

[118] *See id.*

legal guardian, in order for their genetic data to be collected, analyzed, retained, or disclosed.[119] The statute further states "a DNA sample and the results of a DNA analysis performed on the sample are the exclusive property of the person sampled or analyzed."[120]

This statute also sets forth penalties for any violation in the collection, storage, or use of an individual's genetic information.[121] Anyone who violates the rules set forth in this law could be liable for up to $5,000 in damages to any person who suffered harm, and liable for up to $100,000 in damages to any person who suffered harm if the violation "resulted in profit or monetary gain to the violator."[122] A violator of this law could also be charged with the crime of "unlawful DNA collection, analysis, retention, or disclosure," which is a class A misdemeanor.[123] A person found guilty of a class A misdemeanor could face up to one year in jail and a fine of $10,000.[124]

The only foreseeably-desired safeguard that is not granted to Alaskan citizens by this genetic privacy statute is protection from unauthorized use of an individual's genetic information by law enforcement. The prohibitions of the Alaskan statute do not apply to "DNA samples collected . . . for a law enforcement purpose, including the identification of perpetrators and the investigation of crimes and the identification of missing or unidentified persons or deceased individuals."[125] The statute does not include any statement of legislative intent describing why the law expressly excludes DNA samples collected for a law enforcement purpose. But this exception is unlikely to change at any point in the near future, because, as mentioned in Section III, companies like Parabon have resolved unfinished police cases through law enforcement use of DNA. These recent successes are unlikely to alter the Alaskan legislature's stance

---

[119] *Id*.
[120] *Id.*
[121] § 18.13.020.
[122] *Id.*
[123] § 18.13.030.
[124] *See* Ave Mince-Didier, *Alaska Misdemeanor Crimes by Class and Sentences*, NOLO, https://www.criminaldefenselawyer.com/resources/alaska-misdemeanor-crimes-class-and-sentences.htm (last visited Jan. 19, 2019).
[125] § 18.13.010.

on whether genetic privacy of an individual is protected when police collect a DNA sample for police purposes.

The Alaskan genetic privacy statute also defines "DNA analysis" as "DNA or genetic typing and testing *to determine the presence or absence* of genetic characteristics in an individual."[126] It further defines a "genetic characteristic" as "a gene, chromosome, or alteration of a gene or chromosome that may be tested to determine the existence or risk of a disease, disorder, trait, propensity, or syndrome, or to identify an individual or a blood relative."[127] Ancestry does not necessarily test for the presence or absence of a risk for disease, disorder, trait, etc.[128] It does, however, provide results about a consumer's "genetic ethnicity estimates and . . . potential DNA matches, linking [the consumer] to others who have taken the AncestryDNA test."[129] These results are produced from Ancestry's analysis of the consumer's autosomal DNA, which includes almost all of the twenty-two pairs of non-sex chromosomes.[130] Here, the definition of "DNA analysis" would bring Ancestry within the scope of the law because the company's DTC genetic testing kit analyzes chromosomes to determine the existence of a certain trait (ethnicity, risk for disease, etc.) and to identify a potential relative.

The Alaskan genetic privacy statute vests property rights in an individual to their own DNA sample and genetic information. The law also sets forth a civil and criminal penalty for anyone who misuses another's DNA sample or genetic information. With the expansive definition of "DNA analysis" in the statute, Ancestry would be required to abide by the statute if it were in Alaska's jurisdiction. This is an idealistic genetic privacy law upon which a new federal statute should be based in order to provide United States citizens with as much protection as possible from having their genetic information used against them.

---

[126] *See* § 18.13.100 (emphasis added).

[127] *Id.*

[128] *See* ANCESTRYDNA, ANCESTRYDNA 101: THE INSIDER'S GUIDE TO DNA, *supra* note 8.

[129] *Id.*

[130] *See id.*

2. *New Mexico*

In 2015, New Mexico enacted its Genetic Information Privacy Act ("GIPA").[131] GIPA defines genetic information as "information about the genetic makeup of an individual or members of an individual's family, including information resulting from genetic testing, genetic analysis, DNA composition, participation in genetic research or use of genetic services."[132] GIPA's definition for "genetic analysis" includes chromosomal analysis, which tests for "a propensity for or susceptibility to illness, disease, impairment or other disorders."[133]

GIPA requires informed and written consent of an individual in order to collect, store, or disclose the individual's genetic information.[134] But GIPA also provides a laundry list of exceptions to this rule.[135] The most interesting of these exceptions is one that

---

[131] N.M. STAT. ANN. § 24-21-1 (West 2019).

[132] § 24-21-2.

[133] *Id.*

[134] § 24-1-3.

[135] *Id.* Subsection (C), entitled "Genetic Analysis Prohibited without Informed Consent; Exceptions," states:

> An individual's DNA, genetic information or the results of genetic analysis may be obtained, retained, transmitted or used without the individual's written and informed consent pursuant to federal or state law or regulations only:
> (1) to identify an individual in the course of a criminal investigation by a law enforcement agency;
> (2) if the individual has been convicted of a felony, for purposes of maintaining a DNA database for law enforcement purposes;
> (3) to identify a deceased individual;
> (4) to establish parental identity;
> (5) to screen newborns;
> (6) if the DNA, genetic information or results of genetic analysis are not identified with the individual or the individual's family members;
> (7) by a court for determination of damage awards pursuant to the Genetic Information Privacy Act;
> (8) by medical repositories or registries;
> (9) for the purpose of medical or scientific research and education, including retention of gene products, genetic information or genetic analysis if the identity of the individual or the individual's family members is not disclosed;

allows for the unauthorized use, storage, and disclosure of a person's genetic information for the purpose of research and education.[136] GIPA requires that the identity of the individual or their family not be disclosed if their genetic information is used without authorization in this circumstance,[137] but if someone still objects, there is an exception to the exception which prohibits that unauthorized use.[138] An individual, or representative of that individual, is allowed to object on the basis of "religious tenets or practices" to any unauthorized collection, storage, disclosure, or use allowed under paragraphs 5, 8, 9, 10, and 11 of subsection (C).[139] GIPA also prohibits use of genetic information to discriminate in insurance, employment, housing, or lending situations.[140] In addition, GIPA provides that no one shall retain another's genetic information or DNA sample without first obtaining written consent from the individual.[141]

There are established penalties for anyone who does not abide by GIPA, but the penalties are limited to civil actions.[142] The attorney general, district attorney, or a person whose rights under GIPA were violated all have the ability to bring a civil action against a violator of GIPA.[143] An injured individual is eligible to receive actual damages, attorney fees, court costs, and up to $5,000 of damages in addition to any economic loss if the violation was caused by willful or grossly negligent conduct.[144] Each separate occurrence

---

> (10) for the purpose of emergency medical treatment consistent with applicable law; or
>
> (11) by a laboratory conducting an analysis or test of a specified individual pursuant to a written order to the laboratory from a health care practitioner or the health care practitioner's agent, including by electronic transmission.

Id.

[136] *Id.*

[137] *See id.*

[138] § 24-21-3.

[139] *See id.*

[140] § 24-21-4.

[141] § 24-21-5.

[142] § 24-21-6.

[143] *See id.*

[144] *See id.*

of wrongful collection, storage, disclosure, or use of genetic information is treated as an actionable violation of GIPA.[145]

The New Mexico genetic privacy law is well-rounded, but does not protect the consumer of a DTC genetic testing kit from misuse as well as Alaska's genetic privacy act. The scope of GIPA includes DTC genetic test kit companies like Ancestry because the statutory definitions of "genetic information" and "genetic analysis" include autosomal analyses and the results thereof, which Ancestry conducts. GIPA does offer individuals the right to retain their DNA and genetic information, but it does not classify either as the individual's personal property.[146] GIPA attempts to prohibit unauthorized collection, disclosure, and use of genetic information, but attaches a long list of exceptions to that rule.[147] The Act offers a unique religious objection to unauthorized use of a person's genetic data, but the statute never defines what qualifies as "religious tenets or practices." It is unclear whether this religious exemption will be as low of a hurdle as some of the religious exemptions allowed by state vaccine laws, which are notorious for being exploited by non-religious people.[148] Further, GIPA does not include criminal penalties for violations, but the statute is proactive enough to distinguish that each instance of wrongful conduct is a separate and actionable violation of the law which can result in a civil penalty.[149] This could add up for a company such as Ancestry if there were a case of mass misuse of genetic information among the considerable amount of personal data they store.

---

[145] *Id.*

[146] *See* § 24-21-3.

[147] *See id.*

[148] *See* Martha Quillin, *Thousands of NC Students Aren't Vaccinated – All Because of This Easy Exemption*, NEWS & OBSERVER (Apr. 25, 2018), https://www.newsobserver.com/news/politics-government/article188633004.html; *see also* N.C. GEN. STAT. § 130A-157 (2018) ("If the bona fide religious beliefs of an adult or the parent, guardian or person in loco parentis of a child are contrary to the immunization requirements contained in this Chapter, the adult or the child shall be exempt from the requirements . . . [u]pon submission of a written statement . . . .")

[149] *See* § 24-21-6.

3. *Maryland*

In 1997, the legislature of Maryland passed the first draft of its only statute pertaining to genetic privacy, titled "Use of Genetic Tests to Affect Terms or Conditions of Health Insurance Policies or Contracts Prohibited."[150] The most recent version of this statute became effective in 2011 and remains narrow in scope of restrictions upon disclosure of genetic information.[151] This statute consists of regulations in two subsections: (1) the use of genetic tests to affect terms or conditions of health insurance policies and (2) disclosure of identifiable genetic information to authorized employees or health care providers.[152] The first subsection of the statute is prefaced with a statement that it does not apply to life insurance policies, annuity contracts, long-term care insurance policies, or disability insurance policies.[153] Next is a statement that prohibits insurers, nonprofit health service plans, and health maintenance organizations from using genetic information to influence the terms, conditions, or price of a health policy or contract.[154] This section also prohibits the release of genetic information without the concerned individual's written consent.[155] The second subsection of the statute

---

[150] MD. CODE ANN., INS. § 27-909 (West 2019).

[151] *See id.*

[152] *Id.*

[153] *Id.*

[154] *Id.*

[155] *Id.* The full text of this subsection is as follows:

> An insurer, nonprofit health service plan, or health maintenance organization may not:
>
> (1) use a genetic test, the results of a genetic test, genetic information, or a request for genetic services, to reject, deny, limit, cancel, refuse to renew, increase the rates of, affect the terms or conditions of, or otherwise affect a health insurance policy or contract;
>
> (2) request or require a genetic test, the results of a genetic test, or genetic information for the purpose of determining whether or not to issue or renew health benefits coverage; or
>
> (3) release identifiable genetic information or the results of a genetic test to any person who is not an employee of the insurer, nonprofit health service plan, or health maintenance organization or a participating health care provider who provides medical services to insureds or enrollees without the prior written authorization of the individual from whom the test results or genetic information was obtained.

Id.

limits disclosure of identifiable genetic information to an authorized employee or health care provider only to situations in which (1) a patient needs medical care, or (2) for the purpose of conducting legal, board-approved research.[156]

The definitions in this statute are far more constricted than those of the Alaska statute.[157] "Genetic information" is defined as information:

> 1. about chromosomes, genes, gene products, or inherited characteristics that may derive from an individual or a family member; 2. obtained for diagnostic and therapeutic purposes; *and* 3. obtained at a time when the individual to whom the information relates is asymptomatic for the disease.[158]

"Genetic information" does not include regular physical measurements; clinical analyses of blood, urine, or chemicals; drug tests; or human immunodeficiency virus (HIV) tests.[159]

Violation of the Maryland statute does not lead to any civil action or criminal penalty against an individual.[160] But if a violator is an insurance company, they may receive a cease-and-desist order which commands the insurer to immediately shut down all insurance writing the company performs in the state of Maryland.[161] As mentioned earlier, this Maryland statute does not place many limits on the collection, storage, or use of an individual's genetic information.[162] The purpose of the legislation was to regulate and prevent deceptive practices in the business of insurance.[163] This was intended to keep insurance providers from benefitting through discriminatory methodologies such as fixing the policy rates at a higher price for someone who is moderately overweight and refusing to come down on the price until that person provides a

---

[156] *Id.*
[157] *See id.*
[158] *Id.*
[159] *Id.*
[160] *Id.*
[161] *Id.*; *see also* § 4-114 (providing for issuance of a cease-and-desist order of anyone found in violation of the Maryland genetic privacy law).
[162] *See* § 27-909.
[163] *See* § 27-101.

genetic screening result that shows no genetic predisposition to diabetes.

The statute could, however, give insurers flexibility to employ deceptive practices in making insurance transactions. For example, an insurance provider could discriminately request that a healthy man produce a genetic screen for any theoretical genetic susceptibility to one of the enumerated exclusions to "genetic information."[164] This deceptive practice could easily carry over to the DTC genetic testing industry under this statute because it provides for no regulation of collection, storage, or use of genetic information outside the realm of insurance practices. Under Maryland's only genetic information privacy act, genealogy companies such as Ancestry are yet again left to regulate their own handling of consumer's DNA.

V. THE VISION: A PROPOSITION TO PREVENT MISUSE OF DNA SAMPLES AND GENETIC INFORMATION

A new, all-encompassing federal statute is necessary to bring DTC genetic test kit companies within the scope of uniform regulation. As laws across the United States currently stand, some states can regulate Ancestry's actions with respect to genetic information, some states can only regulate genetic information in a health care and insurance context, and almost half of the states provide no guidance at all on a citizen's genetic privacy rights. This incoherence amongst the states provides DTC genetic test kit companies an advantage over their consumers. The companies can implement choice-of-law clauses in their terms and conditions to preemptively apply law from a state with little or no regulation of genetic privacy.[165] This in turn allows these companies broader collection, storage, disclosure, and use rights of consumers' genetic information without fear of any liability. In fact, Ancestry has

[164] For purposes of this example, the genetic screen is testing for information not included within GINA's definition of genetic information.

[165] John F. Coyle, *The Canons of Construction for Choice-of-Law Clauses*, 92 WASH. L. REV. 631, 634 (2017) (observing that sophisticated contracting parties, such as insurance companies, may research laws of multiple jurisdictions and draft a choice-of-law clause that incorporates the law most favorable to the sophisticated party).

specified Utah as the state law which governs all terms and uses of its service for consumers within the United States.[166] Interestingly enough, Utah's genetic privacy laws only prohibit the misuse of genetic information in employment and insurance contexts, leaving DTC genetic test kit companies unregulated.[167] A federal law would provide uniformity in genetic privacy laws across the country and prevent DTC genetic test kit companies from forum-shopping for states that would provide little to no penalty at all for misuse of genetic information.

This federal law must also effectively regulate DTC genetic test kit companies. An effective federal law would be one that is not too narrow in scope and regulates all of a person or entity's interactions with another's genetic information: collection, storage, *and* use. The scope of the law should not be confined to insurance providers for the purpose of defeating deceptive practices. The reach of the law should extend to any person, company, or government entity that has an initial interaction with a person's genetic information outside of the ordinary course of medical interactions or law enforcement operations where acquisition of genetic information is routine. The effective law would not infringe on medical or law enforcement professionals' ability to execute their ordinary business with DNA samples and genetic information they produce. But the law would prohibit those professionals, and any other person, from collecting, storing, or using DNA samples and genetic data that they did not produce—such as those found on genealogy sites, like Ancestry, or on compilation databases, like GEDmatch.[168]

An effective federal law would prohibit the initial collection, continued storage, or prolonged use of a person's genetic information without the concerned individual's informed and written consent. In addition, it would vest personal property rights of DNA and DNA samples in the fabricator of said DNA or DNA sample. This would ensure a DTC genetic testing kit consumer has

---

[166] *See Ancestry Terms and Conditions*, ANCESTRYDNA (June 5, 2018), https://www.ancestry.com/cs/legal/termsandconditions.

[167] *See State Genetic Privacy Laws*, *supra* note 109; *see also* UTAH CODE ANN. §§ 26-45-101 to -106 (West 2019) (providing statutory penalties and civil rights of action for misuse of genetic information by only employers and insurers).

[168] *See* Snow & Schuppe, *supra* note 51.

greater control over his own voluntarily-submitted sample, rather than just trusting the company will abide by their privacy policy and return the sample and other information when asked. In order to ensure DNA samples are returned to their rightful owners, the ideal law would provide a right of retention to the person from whom the DNA was produced.

In the event a DTC genetic test kit company does misuse DNA samples or genetic information, a suitable federal law must also provide effective deterrence and discipline. Each individual instance of genetic information misuse should constitute a separate and actionable violation of the statute. Each violation of the statute should provide for both civil (money damages) and criminal (jail time and fine) liability. DNA samples and genetic information are highly valuable in today's world; the law should treat them as such.

Lastly, a desirable federal genetic information privacy act prohibits disclosure, acquisition, or use of a person's genetic sample or information by law enforcement without the concerned individual's informed consent. The interests of law enforcement must be balanced with the interests of the public, similar to the ideology behind the Maryland bill proposed by Charles Sydnor. Law enforcement has an interest in using all available resources that may lead to the identification and apprehension of criminals.[169] The DTC genetic test kit users have an interest in maintaining the privacy of their genetic information. The United States' Constitution grants citizens a right against unreasonable searches and seizures, as well as protection from warrants issued without probable cause.[170] The government should abide by that policy by further protecting its citizens' genetic information from warrantless and unauthorized use by third parties.

VI. CONCLUSION

While it is laudable that DTC genetic testing companies, such as Ancestry, are implementing privacy policies with self-imposed limitations on handling of consumers' genetic information, it is important to remember that those companies are still businesses.

[169] *See* Watts, *supra* note 67.
[170] *See* U.S. CONST. amend. IV.

Businesses exist to make profit, and genetic information holds near infinite opportunity for profit.[171] The need for a uniform, all-encompassing federal law that regulates collection, storage, disclosure, and use of genetic information is mounting in urgency as DTC genetic testing kits rise in popularity. These genetic testing kit companies collect, store, and use Americans' DNA without much federal oversight. A little over half of states have already recognized the threat to their citizens' safety and enacted legislation towards limiting the manners in which a concerned individual's DNA could be used against them. The potential for discrimination by an insurer, unauthorized distribution of a DNA sample, or unrestricted access to DNA by law enforcement exemplify the need for immediate implementation of an updated federal genetic information privacy act. Protection from discrimination alone through genetic information is no longer sufficient protection.

The discrepancies between the three state statutes discussed in this article provide a sampling of the variance among all twenty-six current state laws concerning genetic information privacy. This lack of uniformity allows companies such as Ancestry to "shop" for a jurisdiction with more passive laws regarding the handling of genetic information, lessening the likelihood Ancestry could be found liable under any statute were the company to misuse genetic information. An effective federal law would create uniform law in all fifty states, preventing companies from forum-shopping for a way to legally exploit sensitive data. An effective federal genetic privacy law would deter, discipline, and hold DTC genetic test kit companies accountable for any misuse of consumers' genetic material.

---

[171] *See, e.g.*, Michael Grothaus, *How 23andMe is Monetizing Your DNA*, FAST CO. (Jan. 5, 2015), https://www.fastcompany.com/3040356/what-23andme-is-doing-with-all-that-dna (reporting a sixty million dollar deal 23andMe acquired by offering up data from members of its Parkinson's disease community).